СИСТЕМА АНАЛІЗУ ЗАГРОЗ ЦИВІЛЬНІЙ БЕЗПЕЦІ: ПУБЛІЧНО-УПРАВЛІНСЬКИЙ АСПЕКТ

SYSTEM OF ANALYSIS OF CIVIL SECURITY THREATS: PUBLIC ADMINISTRATIVE ASPECT

УДК 351.862
DOI https://doi.org/10.32782/pma2663-5240-2023.35.35

Кривошликов С.Ф.
кандидат технічних наук,
ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», доцент кафедри національної безпеки Інституту безпеки, м. Київ, Україна,
kryvoshlykov_sergii@ukr.net
ORCID ID: https://orcid.org/0009-0008-5494-8880

Тимошенко О.О.
кандидат економічних наук,
Фінансова компанія «Онлайн Фінанс», директор
м. Київ, Україна
adbezpeka@gmail.com
ORCID ID: https://orcid.org/0009-0001-8227-8772

Стаття присвячена дослідженню системи аналізу загроз цивільній безпеці, з особливим акцентом на публічно-управлінському аспекті. У сучасних умовах, коли кількість та різноманітність загроз зростає, важливою складовою національної безпеки є захист населення від надзвичайних ситуацій, таких як природні катастрофи, техногенні аварії та терористичні акти. Основною метою дослідження є розгляд методів і інструментів, що використовуються державними органами для ідентифікації, оцінки та управління загрозами. Автори аналізують структуру та функціонування системи управління цивільною безпекою на різних рівнях, а також досліджують нормативно-правову базу, що регулює цю діяльність.

Акцентовано увагу на важливості комплексного підходу до аналізу загроз, який включає в себе накопичені знання та досвід у цій галузі. Розглянуто, як дані про інциденти, такі як природні катастрофи, техногенні аварії або пожежі, можуть бути перетворені у важливу інформацію для запобігання або зменшення впливу загроз. Методологія, запропонована авторами, базується на найкращих міжнародних практиках та стандартах, що дозволяє здійснювати систематичний та структурований аналіз загроз. Розуміння життєвих циклів різних подій є ключовим для розробки ефективних стратегій цивільного захисту.

Окрему увагу присвячено використанню чотириетапного механізму життєвого циклу для безпекової організації, який включає підготовку, виявлення та аналіз, стримування, викорінення та відновлення, а також після аварійну діяльність. Запропонований підхід дозволяє забезпечити якісно новий рівень реагування на загрози як на організаційному, так і на національному рівнях. Детально розглянуто, як оптимізація переходу між цими етапами може забезпечити безперервний потік критично важливої інформації, що є надзвичайно важливим для ефективного управління цивільною безпекою.

Подальшої уваги заслуговує проблема достовірності інформації про загрози, що вимагає застосування методів пізнання та інструментарію різних наук. Дослідники пропонують приділити особливу увагу оптимізації процесів обміну інформацією між різними етапами життєвого циклу загрози, а також розробці методик підвищення достовірності даних. Важливим напрямом є інтеграція міждисциплінарних підходів для покращення розуміння та прогнозування загроз. Адаптація міжнародних стандартів та практик до національних умов також є перспективним напрямком досліджень, що дозволить підвищити ефективність системи цивільного захисту та забезпечити надійний захист населення в умовах надзвичайних ситуацій.

Ключові слова: *цивільний захист, аналіз загроз, прогнозування, загрози цивільній безпеці, надзвичайні ситуації, розвідка, безпека, публічне управління, джерела загроз.*

The article is devoted to the study of the system of analysis of threats to civilian security, with a special emphasis on the public administration aspect. In today's environment, when the number and diversity of threats is growing, an important component of national security is the protection of the population from emergencies such as natural disasters, man-made accidents and terrorist acts. The main purpose of the study is to examine the methods and tools used by government agencies to identify, assess and manage threats. The authors analyze the structure and functioning of the civilian security management system at various levels, as well as study the legal framework governing these activities.

Attention is focused on the importance of a comprehensive approach to threat analysis, which includes the accumulated knowledge and experience in this area. It is considered how data on incidents, such as natural disasters, man-made accidents or fires, can be transformed into important information to prevent or reduce the impact of threats. The methodology proposed by the authors is based on the best international practices and standards, which allows for a systematic and structured threat analysis. Understanding the life cycles of various events is key to developing effective civil protection strategies.

Particular attention is paid to the use of a four-stage life cycle mechanism for a security organization, which includes preparation, detection and analysis, deterrence, eradication and recovery, and post-emergency activities. The proposed approach allows for a qualitatively new level of response to threats at both the organizational and national levels. The author discusses in detail how optimizing the transition between these stages can ensure a continuous flow of critical information, which is extremely important for effective civilian security management.

Further attention is paid to the problem of the reliability of information about threats, which requires the use of cognitive methods and tools from various sciences. The researchers propose to pay special attention to optimizing the processes of information exchange between different stages of the threat life cycle, as well as to developing methods for improving data reliability. An important area is the integration of interdisciplinary approaches to improve understanding and forecasting of threats. Adaptation of international standards and practices to national conditions is also a promising area of research that will increase the efficiency of the civil protection system and ensure reliable protection of the population in emergencies.

Key words: *civil protection, threat analysis, forecasting, threats to civilian security, emergencies, intelligence, security, public administration, sources of threats.*

Об´рунтування актуальності теми дослідження. У сучасному світі, що характеризується високою динамікою ризиків та загроз, ефективний цивільний захист є не лише важливим, але й життєво необхідним. Гарантування безпеки населення та інфраструктури, в умовах надзвичайних ситуацій, вимагає не лише швидкої реакції на вже існуючі проблеми, але й глибокого розуміння потенційних загроз. Тому, система аналізу загроз стає ключовим елементом стратегічного планування у сфері цивільного захисту. Особливого ж значення це набуває в Україні, де в умовах війни саме від ефективності системи цивільного захисту залежить життя і здоров'я сотень тисяч людей.

Детальний аналіз та формування систематичного підходу до оцінки ризиків, є цілком комплементарними з сучасними методами прогнозування загроз. Такий інструментарій є вкрай важливим для фахівців у галузі цивільного захисту, допомагаючи їм підготуватися до майбутніх викликів та ефективно на них реагувати. Зазначене й обумовлює актуальність дослідження та його цінність не лише для науки публічного управління, а й для практики застосування у галузі цивільного захисту.

Мета дослідження: проаналізувати дієві механізми прогнозування загроз в галузі національної та комерційної безпеки, в контексті перспектив їх застосування у галузі цивільної безпеки.

Основний зміст дослідження. Сучасний набір загроз дуже складний і динамічний. На організації часто впливають джерела загроз різної природи, які використовують різні інструменти, що змінюються щодня. Чергові заходи, які так добре працювали на захисті організації ще вчора, можуть вже не мати можливості запобігти тим самим ризикам наступного дня, у залежності від того, як змінилося не лише середовище, але й сама організація. Завдяки такому складному операційному середовищу, служби цивільного захисту мають бути готові відмовитись від спроб створити пріоритетний перелік речей, які потрібно захищати першочергово, і замість цього спробувати захищати все.

Водночас, такий підхід не є виправданим, з огляду на обмеженість ресурсів [1]. Спеціалісти в аналізі загроз стверджують, що потрібен пріоритетний розподіл матеріальних та нематеріальних активів, які потребують захисту, оскільки існує надто багато об`єктів для захисту та занадто менше заходів, якими їх можна захистити [2]. Навіть у дуже великих організаціях, які мають практично необмежений бюджет для побудови системи безпеки, все одно доводиться конкурувати з іншими організаціями за спеціалістів, а час для всіх завжди був і залишатиметься обмеженим ресурсом [3]. З огляду на це зрозуміло, що організаціям вигідно використовувати вже наявні дані про загрози, які спеціалісти з цивільного захисту отримують, проводячи свою діяльність щодо запобігання ризиків.

Аналогічним чином, процес розвідки загроз може бути краще пристосований для цивільного захисту, якщо спеціалісти використовують заздалегідь зібрані дані. Таке поєднане використання даних про загрози є основою раціональної системи аналізу. Звісно ж, запровадження системи аналізу загроз потребує закріплення адміністративно-правовим шляхом у відповідних документах організацій, що дещо виходить за межі теми публікації. Тому, більш детально зупинимось виключно на практичній стороні питання, а до нормативної повернемося іншим разом.

Варто зазначити, що термін «аналіз даних про загрозу» може мати різне значення в різному контексті, але у даному випадку, метою є розробка загальної системи збору даних з питань загроз цивільній безпеці організацій чи суспільства в цілому [4]. Визначення, надане Тілманом (Craig Tillman), є корисним для розуміння та застосування у найширшому спектрі: «Система аналізу загроз – це організаційна здатність цілісно мислити про загрозу та невизначеність, розмовляти загально-прийнятою мовою загрози, ефективно використовувати перспективні концепції та інструменти загрози для прийняття кращих рішень для знешкодження загроз, розуміти виграш від своїх можливостей і створення стійких пріоритетів» [5]. Дане визначення видається вичерпним, хоч і доволі узагальненим.

Початковий життєвий цикл для безпекової організації, під час виникнення загроз, складається з наступних етапів: 1) підготовка, 2) виявлення та аналіз, 3) стримування, викорінення та відновлення, 4) після аварійна діяльність. По закінченні цього чотири-ступеневого циклу, результати мають повернутися на початок життєвого циклу та до інших життєвих циклів.

Реагування на надзвичайні ситуації – це один із тих процесів, який дуже виграє від належного попереднього планування, і перша фаза наведеного життєвого циклу – «підготовка» – це добре ілюструє. Організація завжди повинна мати ресурси, необхідні для відповідної реакції [3]. Це може включати власну розробку, чи придбання вже наявних корисних технологій, що допоможуть захиститись у випадку реалізації загрози, налашту-

вання обчислювальних активів для забезпечення належних доказів (у випадку настання катастрофи) та встановлення правильних тригерів для попередження населення, коли катастрофа триває. Нарешті, цей крок процесу включає залучення та навчання відповідного персоналу для знання організаційних ресурсів, можливостей та процесів у випадку підтвердженої загрози настання надзвичайної ситуації. Окремої уваги в цьому контексті заслуговують технології форсайту [6]. Вони дозволяють не лише спрогнозувати загрози, але й передбачити їх обсяг та інші особливості.

Другий етап – «виявлення та аналіз», демонструє необхідність організації мати можливість знати, коли небезпечна ситуація розгортається в контрольованому нею середовищі. Це означає наявність спеціалістів та технологій (відповідно до першого етапу), які зможуть моніторити інформацію та аналізувати всі нюанси, щоб визначити пріоритет дій на наступному етапі. Даний етап характеризується відносно високим ступенем помилкових дій, які можуть виникнути в результаті прийняття хибних рішень в ході моніторингу. Як результат, зрілі організації встановлюють пріоритетну рубрику для того, щоб знати, коли їм потрібно швидко реагувати на певні негативні показники. Таке визначення пріоритетів є чудовою можливістю для інтеграції з системою розвідки загроз. Знання правильних пріоритетів, заснованих на оцінці загрози, на цій ранній фазі реагування на надзвичайні ситуації, є критично важливим для належного управління загрозами.

Третя фаза циклу призводить до зупинення надзвичайних ситуацій (як природного, так і техногенного характеру). Вона передбачає як фізичне обмеження розповсюдження проблеми (карантин заражених осіб, локалізація пожежі), так і усунення доступу нових суб'єктів до місця небезпеки (обмеження корисного навантаження на конструкції або недопущення втручання шкідливого програмного забезпечення), а також припинення будь-якого розповсюдження шкоди, яке триває або незабаром настане (оборювання полів, санітарна вирубка лісу на шляху пожежі тощо). Дана фаза також передбачає спробу реанімувати відповідні системи життєдіяльності та відновити їх стан роботи (в ідеалі – на такому рівня, який був до настання шкідливої події). На цьому етапі також слід проводити збір даних в цілому та особливо – доказів, оскільки іноді їх потрібно в подальшому передавати правоохоронним органам або кадровим та юридичним відділам для подальших розслідувань.

Заключна фаза циклу реагування на стихійні лиха, яка охоплює діяльність після виникнення проблемних випадків, передбачає інтеграцію з іншими етапами. У межах цієї фази важливо організувати ретельний збір даних та підготовку отриманої в ході інших фаз інформації для подальшого використання. Це може включати детальний опис події, а також аналітичні висновки про її наслідки для організації. Крім того, ця інформація може включати прогнози, які допоможуть виявити подібні випадки в майбутньому, а також запропонувати подальші дії для запобігання подібним інцидентам.

По суті, цей етап дозволяє перетворити негативні наслідки події на корисну інформацію про загрози, яка може бути використана для подальшого планування. Залежно від потреб організації, можна виключити технічні деталі, але завжди варто включати адміністративно-правовий аспект, що узагальнює подію і транскрибує її у форму своєрідної «повчальної історії», яка допомагає відповідальним фахівцям краще зрозуміти ситуацію. Це також зміцнює довіру до аналітичних рекомендацій щодо запобігання подібним загрозам у майбутньому.

Крім того, така інформація може бути використана як вихідний матеріал для початкової фази реагування, а також для підготовки до майбутніх викликів. Внутрішньо створені дані про загрози можна комбінувати з аналогічною інформацією із зовнішніх джерел, що забезпечує інтеграцію в модель цивільного захисту на наступному життєвому циклі. Процес розвідки інформації про загрози являє собою окремий життєвий цикл.

Автори переконані, що збір інтелектуальної інформації про загрози є процесом двох систем, як це визначив лауреат Нобелівської премії Даніель Канеман у своїй книзі «Мислення швидке і повільне». Він докладно описав види прийняття рішень, які роблять люди, та об'єднав їх у дві категорії [7]. Автори, в свою чергу, пропонують перетворити ці постулати у відповідні адміністративно-правові норми організацій. Перші рішення, швидко приймаються, служать для захисту від шкоди та задовольняють потреби нижчого рівня в «Ієрархії потреб» Абрахама Маслоу [8]. Другі, обдумані рішення, які приходять, як результат витрати часу на розгляд вхідних та вихідних даних, правильного застосування системи для аналізу результатів.

Своєрідною пасткою, яка штовхає нас до перших, швидких рішень, є складність других, обдуманих рішень. Системне мислення настільки просте і швидке, що ми часто застосовуємо його за замовчуванням і це допомагає врятуватися, коли виникає загроза. В найкращому випадку воно може призвести до

неправильного вибору, а в гіршому – до війни, фанатизму та расизму. При цьому, всі розуміють, що розвідка загроз повинна бути продуманим зусиллям, розробленим для усунення упереджень та ретельного аналізу зібраної інформації для досягнення найбільш точного та правильного рішення.

Раціональні підходи до аналізу ризиків, пропонувалися в звітах RAND (від «Research and Development» - «Дослідження і розробка») американської некомерційної організації, яка існує з 1948 року та виконує функції стратегічного дослідницького центру, що працює на замовлення уряду США. RAND співпрацює зі збройними силами США та пов'язаними з ними організаціями у таких галузях як аналіз ризиків, прогнози та розвідувальна діяльність [9]. При цьому, пропоновані цим центром механізми можуть бути адаптовані для прогнозування загроз цивільній безпеці.

Є кілька змінних, які необхідні для вірного моделювання загрози, особливо, коли йдеться про кількісні показники. Використовуючи дані, зібрані у певний час і у певному місці, можна накопичити достатню інформаційну базу для моделювання двох змінних показників, що називаються «Частота подій загроз» (TEF) та «Можливість загроз» (TCap) [9]. Ці дві змінні показники дають нам змогу сформувати модель того, як часто виникають аварії або (якщо мова іде про внутрішній персонал), як часто люди роблять помилки, і яким є потенціал завдання шкоди внаслідок цих факторів.

При цьому, дані з профілю загрози розподіляються між цими двома змінними (TEF і TCap), які використовуються як похідні дані до моделі аналізу загроз із міжнародним позначенням «FAIR». Модель FAIR використовується серед професіоналів аналітики даних та призначена для кількісної оцінки ризику настання надзвичайних ситуацій та прогнозування збитків, з використанням економічних показників [10]. Водночас, якісний профіль загрози можна трансформувати у показник частоти загрозливих подій з плином часу (TEF) та виміру того, на що здатні джерела загрози (TCap). І хоча частота є природною кількісною величиною, можливості в моделі FAIR виражаються через рівень джерела загрози. По суті, ті джерела загроз, які можуть здійснити найбільший вплив з точки зору часу, факторів та ресурсів, мають найважливіше значення для показника TCap. Відтак, всі отримані в ході аналізу показники слід зберігати разом із профілем загроз, щоб організації могли чітко усвідомлювати, які саме загрози є пріоритетними.

Принципи FAIR також передбачають використання інформації про стан контролю та економічний вплив подій на організацію, щоб забезпечити точний аналіз загроз. Повна обробка моделі FAIR виходить за рамки дослідження і заслуговує окремого огляду. Але вкрай важливо зазначити, що FAIR фокусується саме на сценаріях. Тобто, потребує повних даних про збитки, включаючи всю палітру загроз, слабкі сторони організацій та потенційні наслідки. Відповідно, сценарії настання найвищих збитків, можуть бути використані разом із деякими прогнозованими проблемами, і допомогти сформулювати заходи протидії, в певних межах.

Таким чином, кожен з механізмів прогнозування має свої сильні сторони та корисність у різних ситуаціях, що складаються в процесі функціонування системи цивільного захисту. Поєднуючи їх разом, можна сформувати дієву систему прогнозування загроз (якщо не стихійного, то бодай – техногенного характеру), що як враховує інформацію про події, які вже сталися, так і формує ймовірнісні сценарії майбутнього.

На практиці часто існує бар'єр між функцією управління ризиками та операціями проти загроз. Не є виключенням і система цивільного захисту. Відтак, команда управління загрозами потребує налагодження співпраці з командою аналітиків, яка повинна краще розуміти загрози для оцінки ризиків та пріоритетів протидії. Даний механізм потребує як належної організації, так і адміністративно-правового закріплення системи розвідки загроз, як плану співпраці, що передбачає чіткі права та обов'язки звітування для кожної команди. Такий механізм допоможе налагодити співпрацю і створити професійні зобов'язання, які сприятимуть кращій роботі в команді та призведуть до вищої результативності розвідки і аналізу загроз.

Отож, осмислення викликів та перспектив, які виникають у сфері цивільного захисту, загострює важливість не лише глибокого аналізу загроз, але й ефективної комунікації суб'єктів обробки та аналізу інформації в умовах, коли кожна секунда має значення. Лише такі методи дозволяють безпековим організаціям не просто реагувати на надзвичайні ситуації, а й передбачати їх, адаптуючись до потенційних загроз заздалегідь. Завдяки належній адміністративно-правовій координації та налагодженню оперативного обміну даними, можна сформувати ефективну систему прогнозування різних сценаріїв розвитку подій.

Таким чином, впровадження передових практик у сфері аналізу загроз, є ключем до підвищення ефективності роботи організацій у сфері цивільного захисту. Що не тільки

сприяє кращому розумінню загроз цивільній безпеці, але й є основою для формування більш безпечного та стійкого середовища, що відповідає безпековим очікуванням сучасного суспільства.

Висновки і перспективи подальших досліджень. Використання в якості інструментарію цивільної безпеки чотирьох етапного механізму життєвого циклу для безпекової організації (що включає: 1) підготовку, 2) виявлення та аналіз, 3) стримування, викорінення та відновлення, 4) після аварійну діяльність), дозволяє як на організаційному так і на національному рівнях перейти до якісно нового реагування на загрози.

Особливої уваги заслуговує комплексний підхід до аналізу загроз, що включає в себе накопичені знання та досвід у цій галузі. Автори детально пояснюють, як перетворити дані про інциденти, такі як природні катастрофи, техногенні аварії або пожежі, у важливу інформацію, яка може допомогти запобігти загрозам або, принаймні, зменшити їх вплив. Наведений метод базується на найкращих міжнародних практиках та стандартах, що дозволяє здійснювати систематичний та структурований аналіз загроз з урахуванням життєвих циклів різних подій.

Розуміння ключових етапів життєвого циклу загрози, від ідентифікації до локалізації, є надзвичайно важливим для розробки ефективних стратегій цивільного захисту. Відтак, у подальшому, окремої уваги дослідників потребує проблема оптимізації переходу між такими етапами, що має забезпечувати безперервний потік критично важливої інформації. Окремої уваги заслуговує й проблема достовірності такої інформації, що також вимагає застосування методів пізнання та інструментарію різних наук.

ЛІТЕРАТУРА:

1. Асоціація з управління проектами. н.д. «Різниця між «згладжуванням ресурсів» і «вирівнювання ресурсів».» apm.org. 15 липня 2018 року. URL : https://www.apm.org.uk/content/resource-smoothing.

2. Гупта, Акаш. 2017 рік. «Планування ресурсної ємності для гнучких команд». *ПМ*. 19 вересня. URL : https://project-management.com/resou...r-agile-teams/.

3. Gareth Saunders. The challenges of resource management in our Agile team. 9 November 2015. *University of St Andrews*. URL : https://digitalcommunications.wp.st-andrews.ac.uk/2015/11/09/the-challenges-of-resource-management-in-our-agile-team/

4. Agarwal, Ravi; Grassl, Wolfgang; Pahl, Joy (January 2012). "Meta□SWOT: introducing a new strategic planning tool". *Journal of Business Strategy*. 33 (2): 12–21. doi:10.1108/02756661211206708

5. Protecting Communities from Climate Change: Using Portsmouth, *Virginia to Kickstart Global Solutions*. URL : https://www.renre.com/forum/protecting-communities-from-climate-change-leadership-forum-2021/

6. Лисенко С. О. Форсайт безпеки в якості майбутнього заходу організацій. *Наукові перспективи*. 2020. №3 (3) С. 102.

7. Даніель Канеман. Мислення швидке і повільне. Київ, 2017. *Наш формат*. 488 с. ISBN978-617-7279-18-0

8. Hoffman, E. (2022). Ideas That Matter: Humanistic Psychology, Past, Present, and Future. *Journal of Humanistic Psychology*, 0(0). https://doi.org/10.1177/00221678221112135

9. RAND Corporation. Springer P. J. Encyclopedia of Cyber Warfare. *Santa Barbara*, 2017. 400 p. ISBN 978-1-4408-4425-6.

10. Калюжна Н, Алтемеіер Ф. Принципи FAIR для дослідницької інформації: звіт із серії воркшопів. *Ukr. ž. bìbl. ìnf. nauk*. 04, Червень 2021; (7): 128-32. URL: http://librinfosciences.knukim.edu.ua/article/view/233322